Information Security Engineering

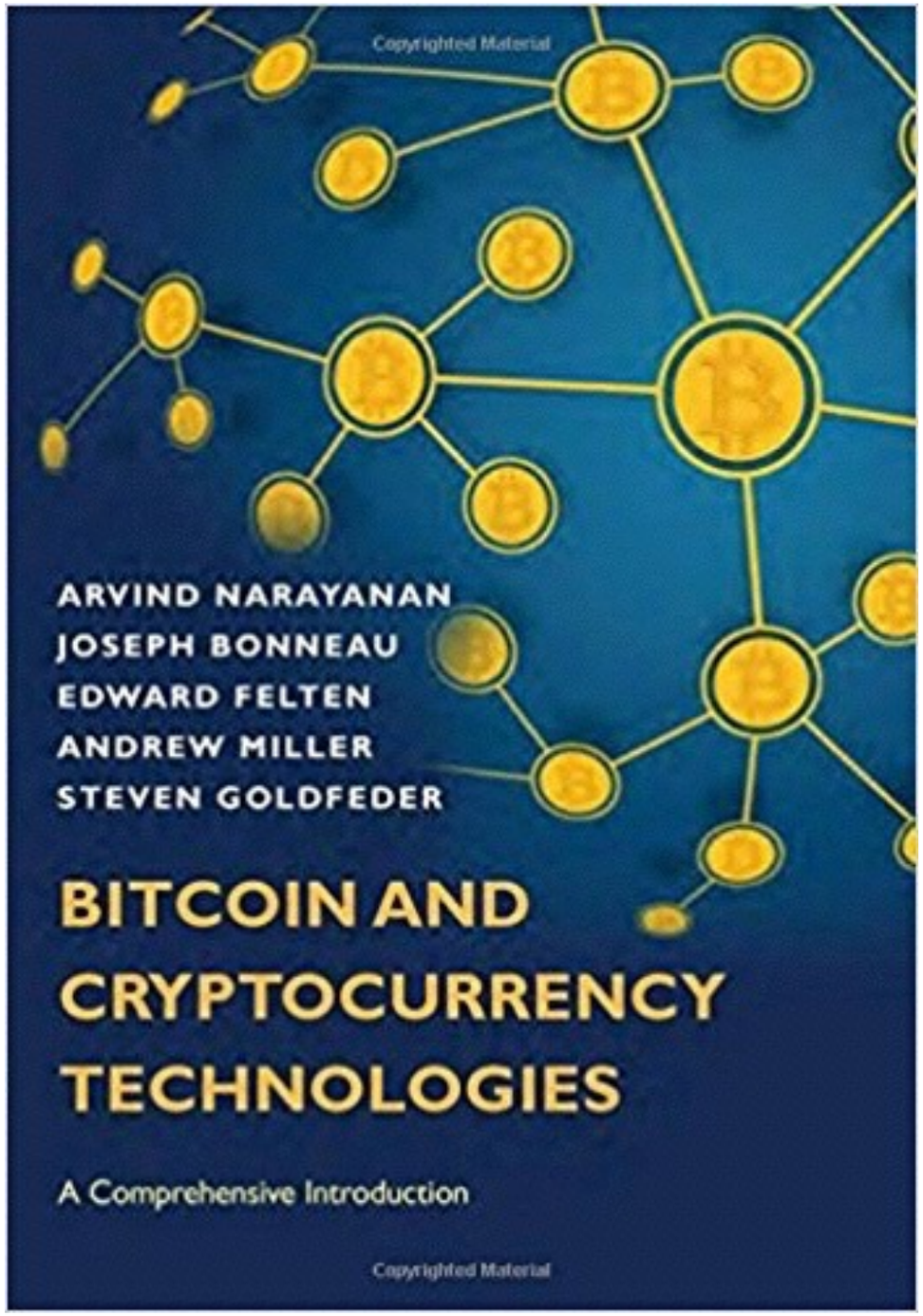
2017.12.06

Bitcoin I

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

参考书


Copyrighted Material
ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER
BITCOIN AND
CRYPTOCURRENCY
TECHNOLOGIES
A Comprehensive Introduction
Copyrighted Material


本页面中的内容受版权保护
BITCOIN
AND
CRYPTOCURRENCY
TECHNOLOGIES
A Comprehensive Introduction


区块链
技术驱动金融
数字货币与智能合约技术
解密区块链，用技术重构金融世界
谢平
肖风
邢早忠
霍学文
刘信义
黄此忠
唐 斌
本页面中的内容受版权保护

主要内容

- **密码学和加密货币**
- 比特币如何去中心化
- 比特币的机制
- 如何存储和使用比特币
- 比特币挖矿
- 比特币和匿名性
- 社区、政治和监管
- 其余挖矿难题
- 比特币作为平台
- 其余代币和加密货币生态系统
- 比特币未来

密码学和加密货币

货币

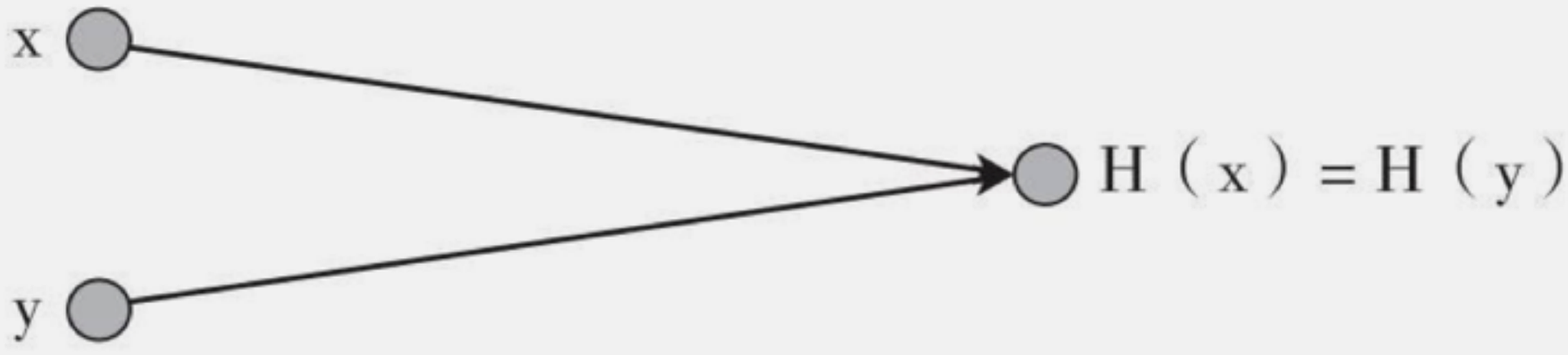
PayPal™

Hash函数

- 输入为任意大小的字符串
- 输出为固定大小，例如256位
- 可以进行有效计算：$O(n)$

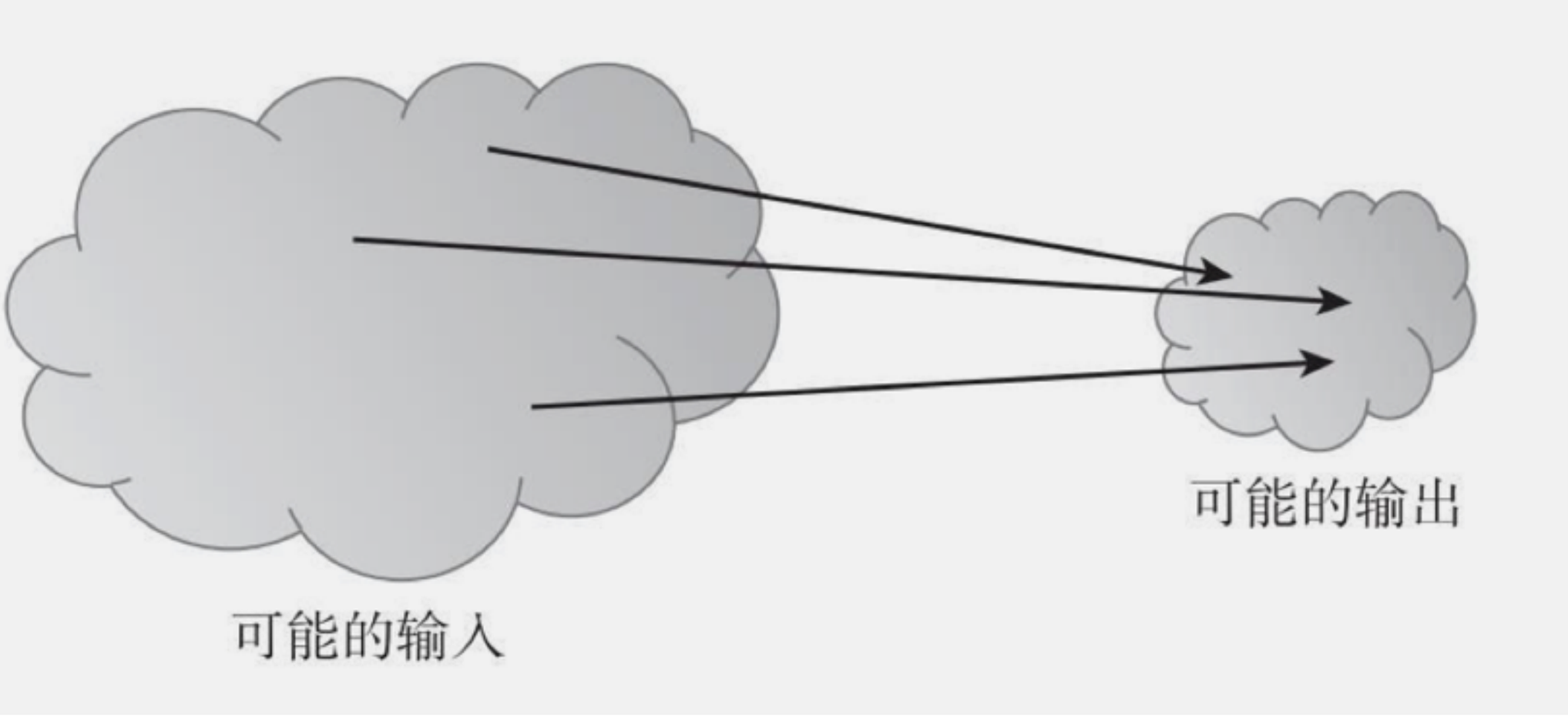
- 抗碰撞
- 隐匿性
- 难题友好

抗碰撞



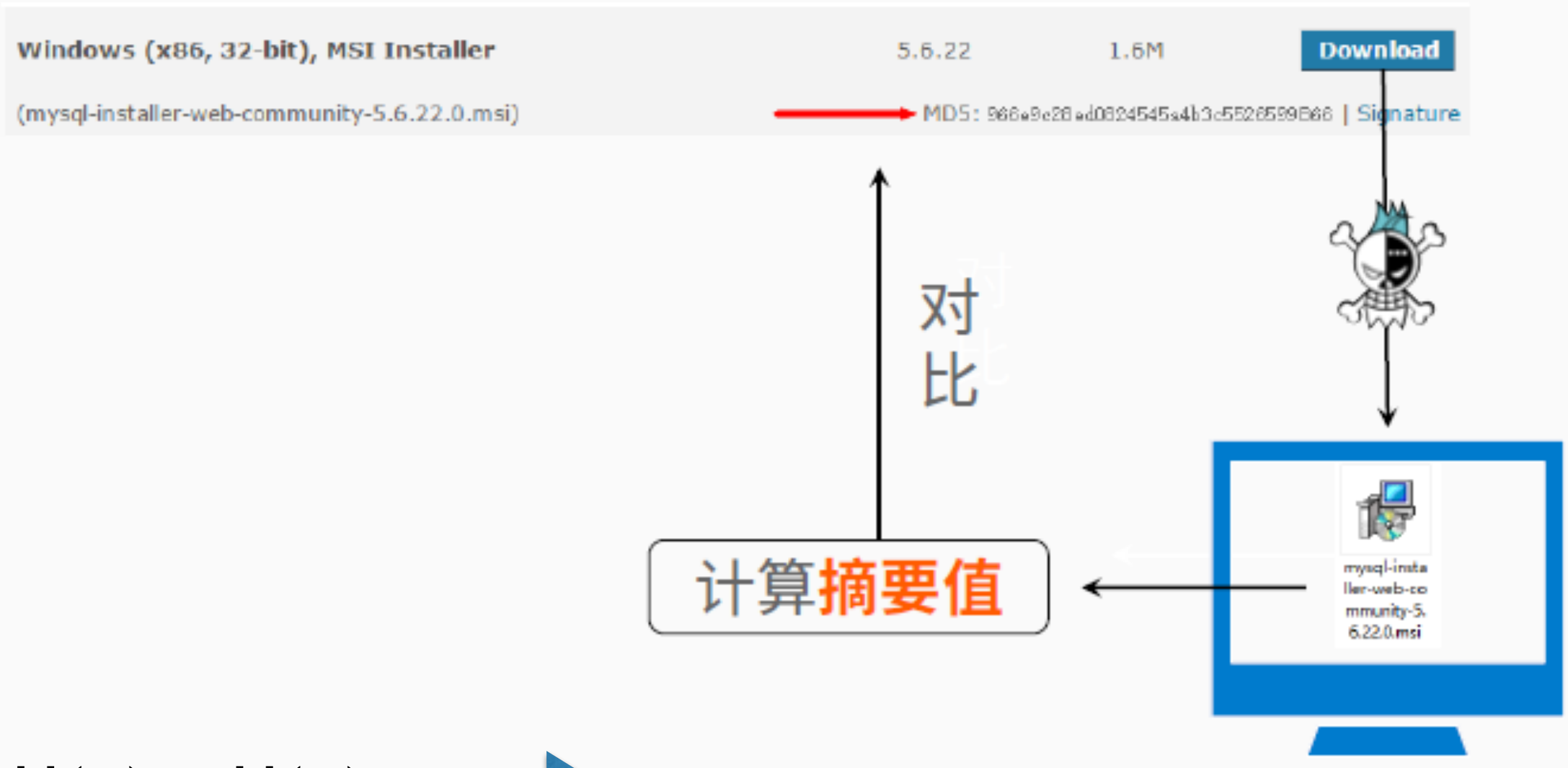
2^{130}

99.8%



应用： Hash作为消息摘要

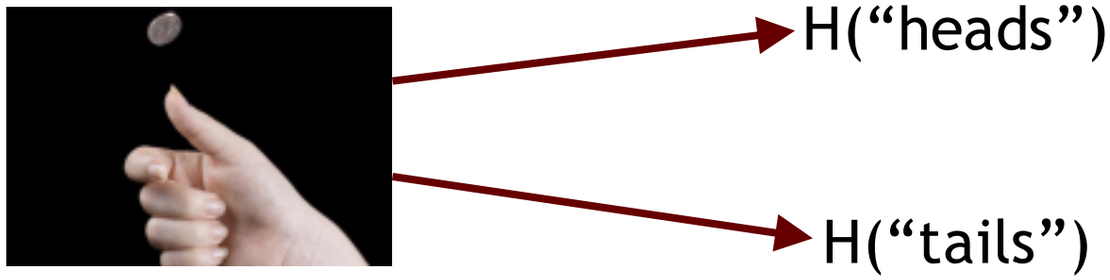
hash足够小



H(x) = H(y) → x = y

隐匿性

- 给出$H(x)$，不能找到x



- 如果概率分布有高的最小熵，非常分散，则具有隐匿性

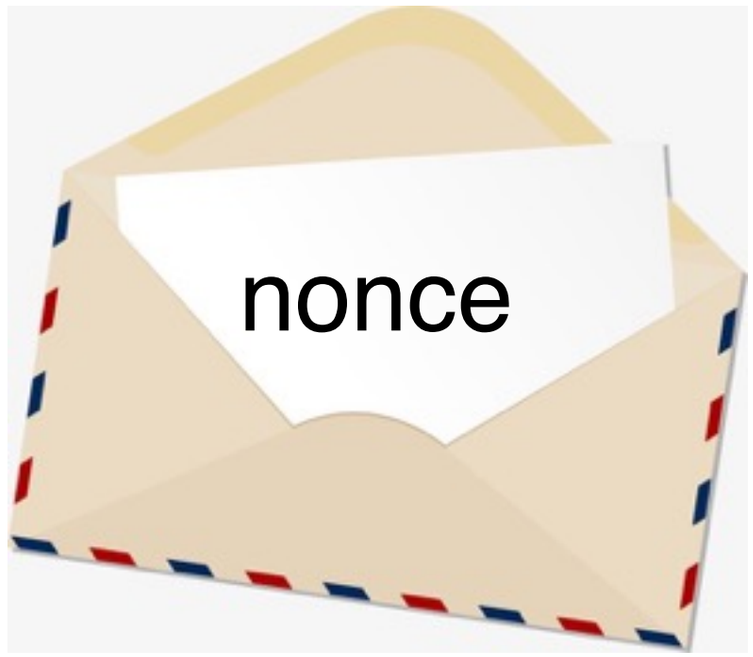
隐匿性应用: 承诺

com := commit(*msg*, *nonce*)

公开*msg*

match := verify(*com*, *nonce*, *msg*)

公开*key*和*msg*



已知com，不能找到*msg*

不能找到*msg!=msg'*, 但*commit(msg,nonce)* == *commit(msg',nonce')*

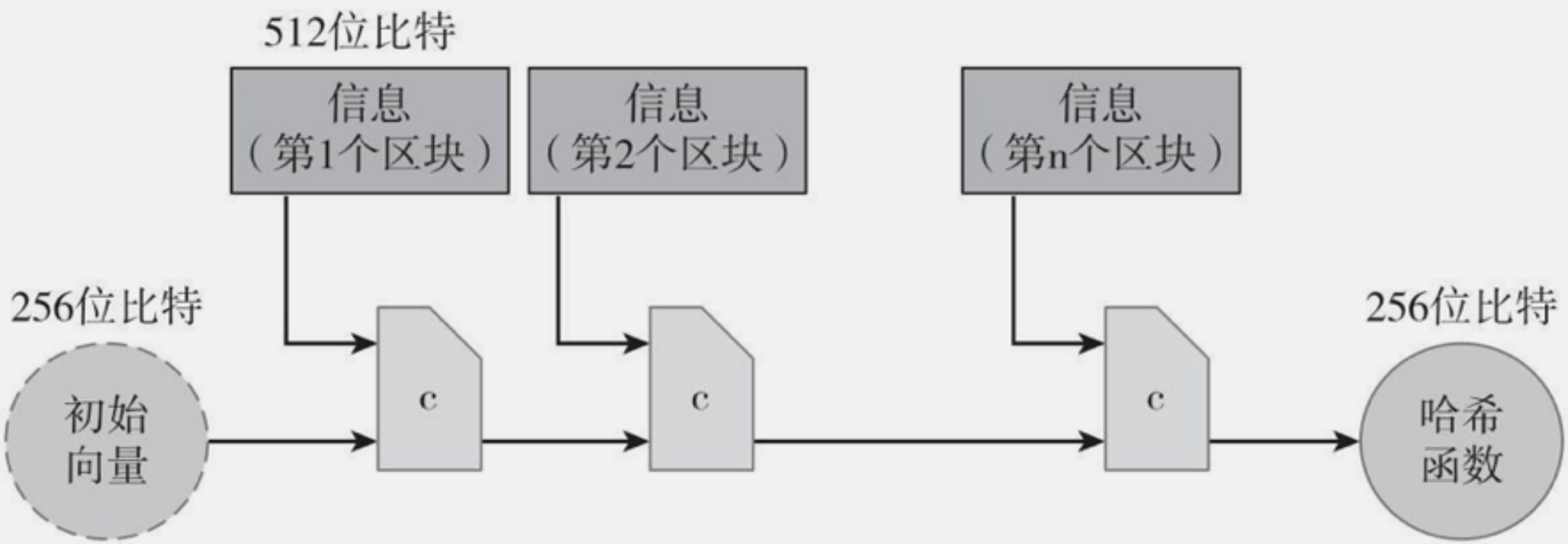
---

commit(*msg)* := (H(*nonce* | *msg*), H(*nonce)*)

verify(*com*, *nonce*, *msg*) := (H(*nonce* | *msg)* == *com*)

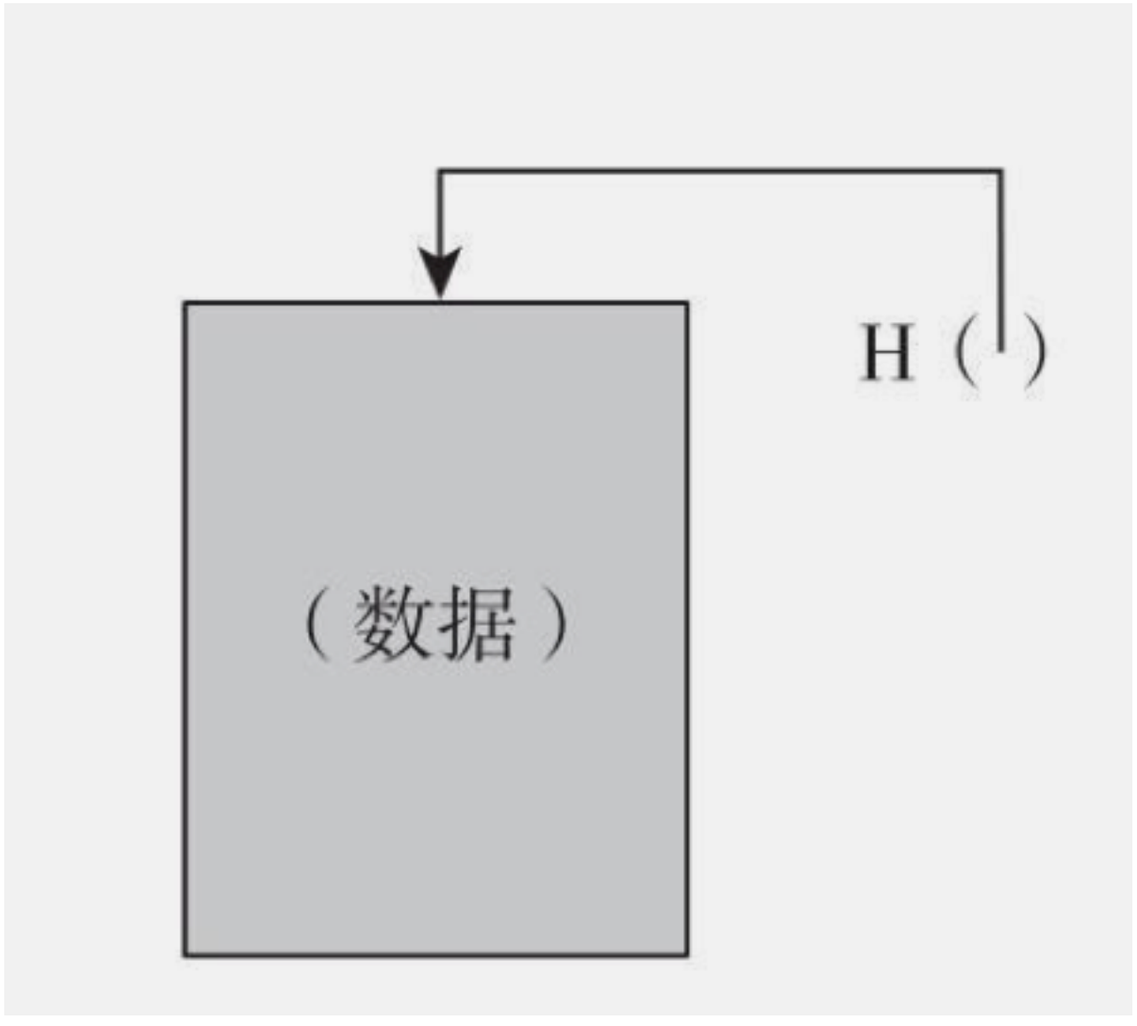
难题友好

SHA-256


512位比特
信息
（第1个区块）
信息
（第2个区块）
信息
（第n个区块）
256位比特
初始
向量
c
c
c
256位比特
哈希
函数

Hash指针

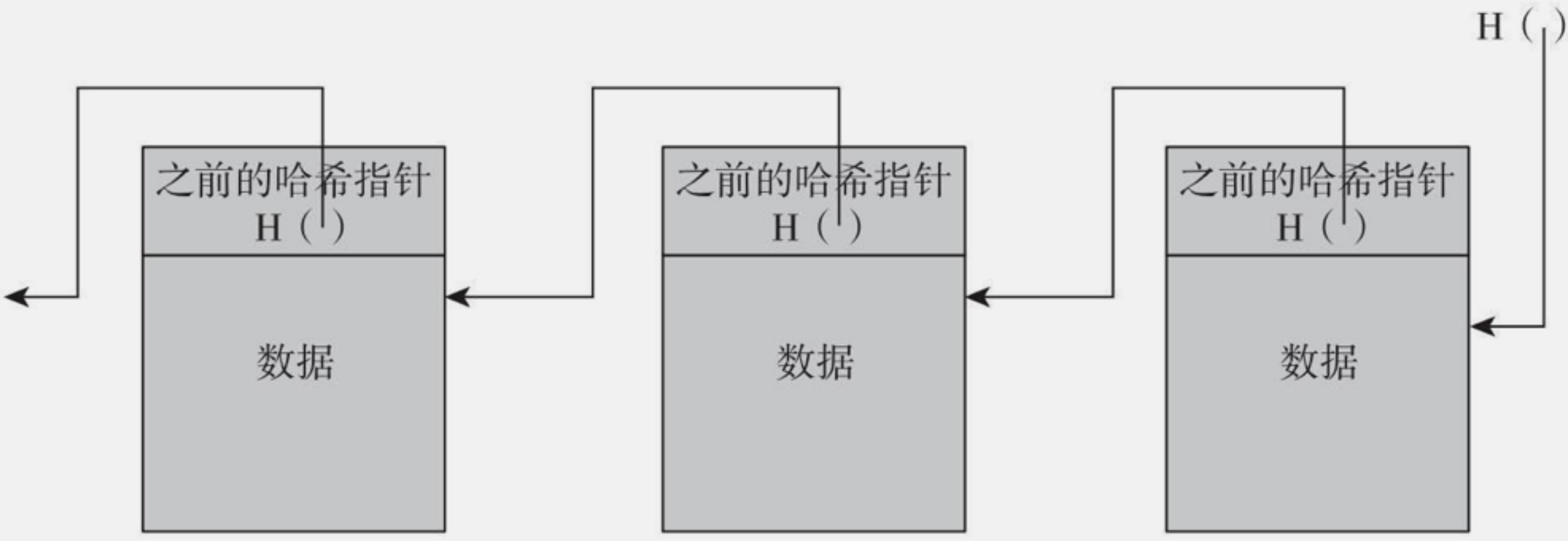
- *Hash*指针是一个指向存储数据及其数据*Hash*的指针



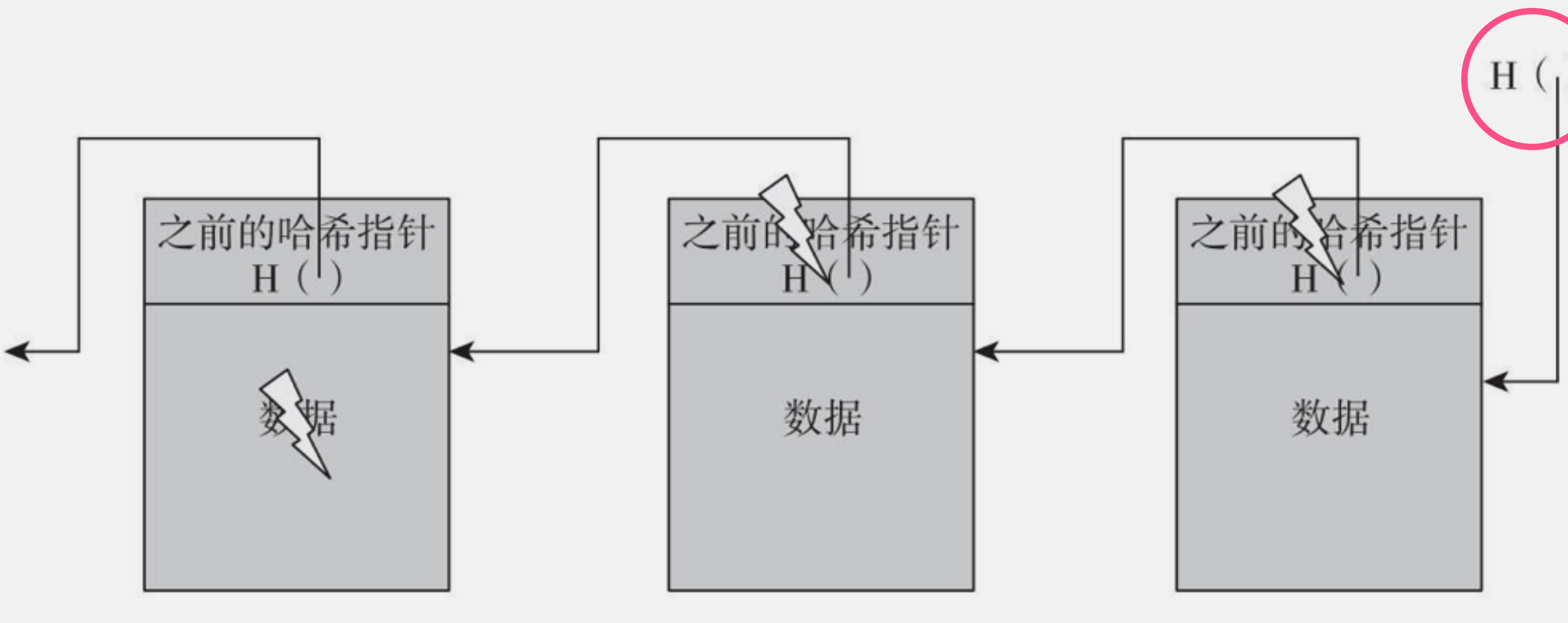
- 取回数据
- 验证数据是否改变

- 区块链的关键思想

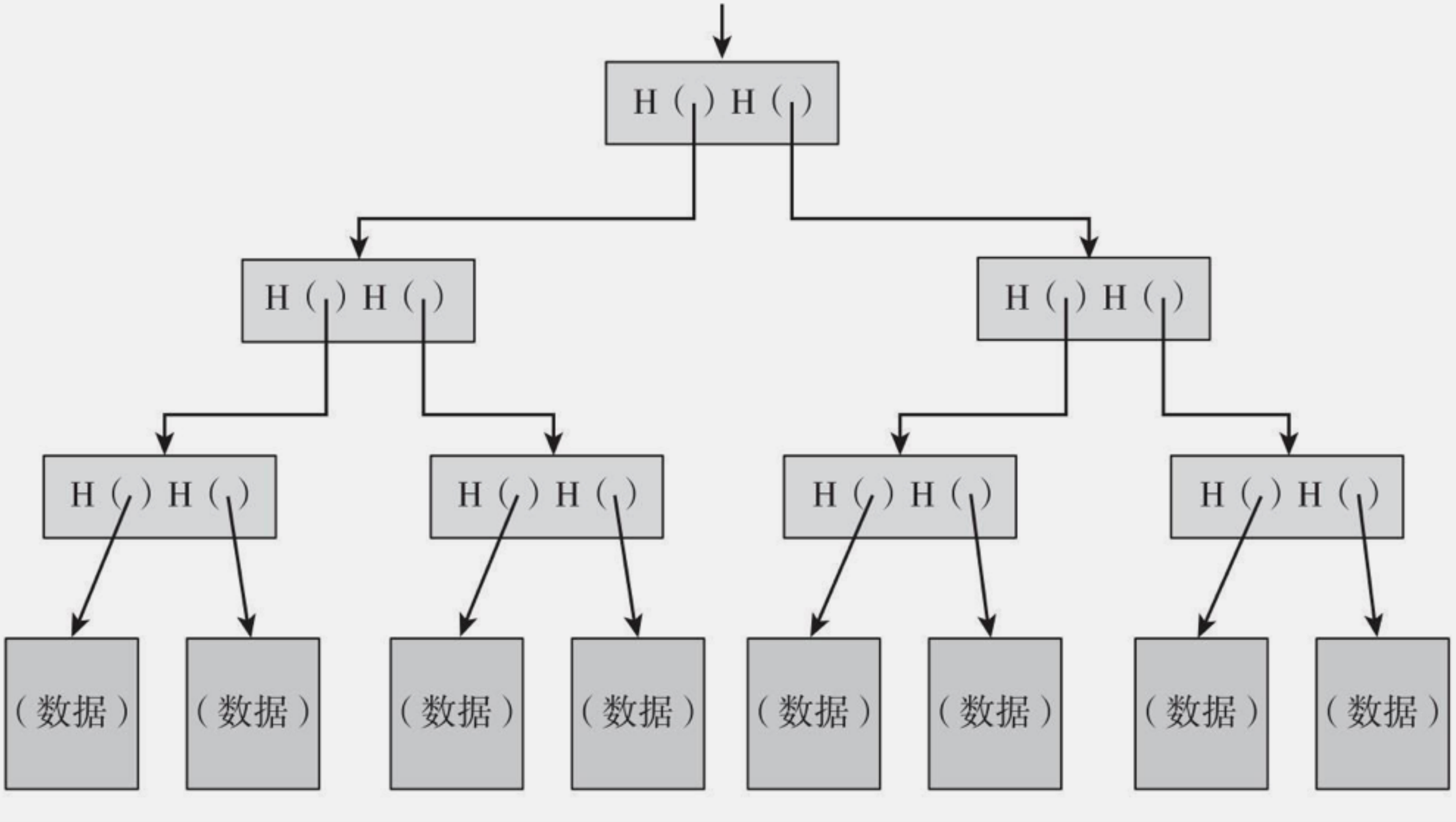
区块链



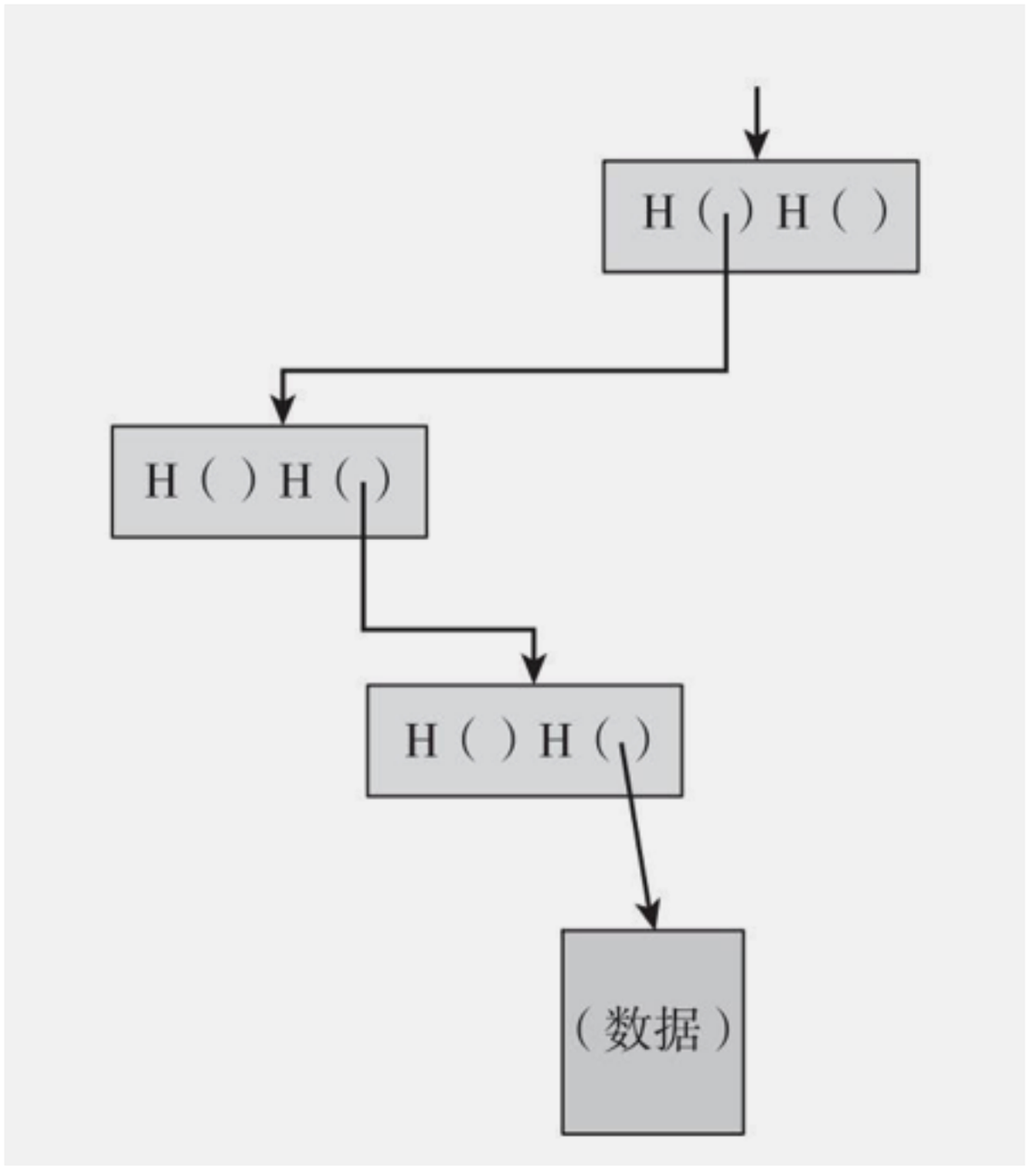
防止篡改



梅克尔树



成员证明

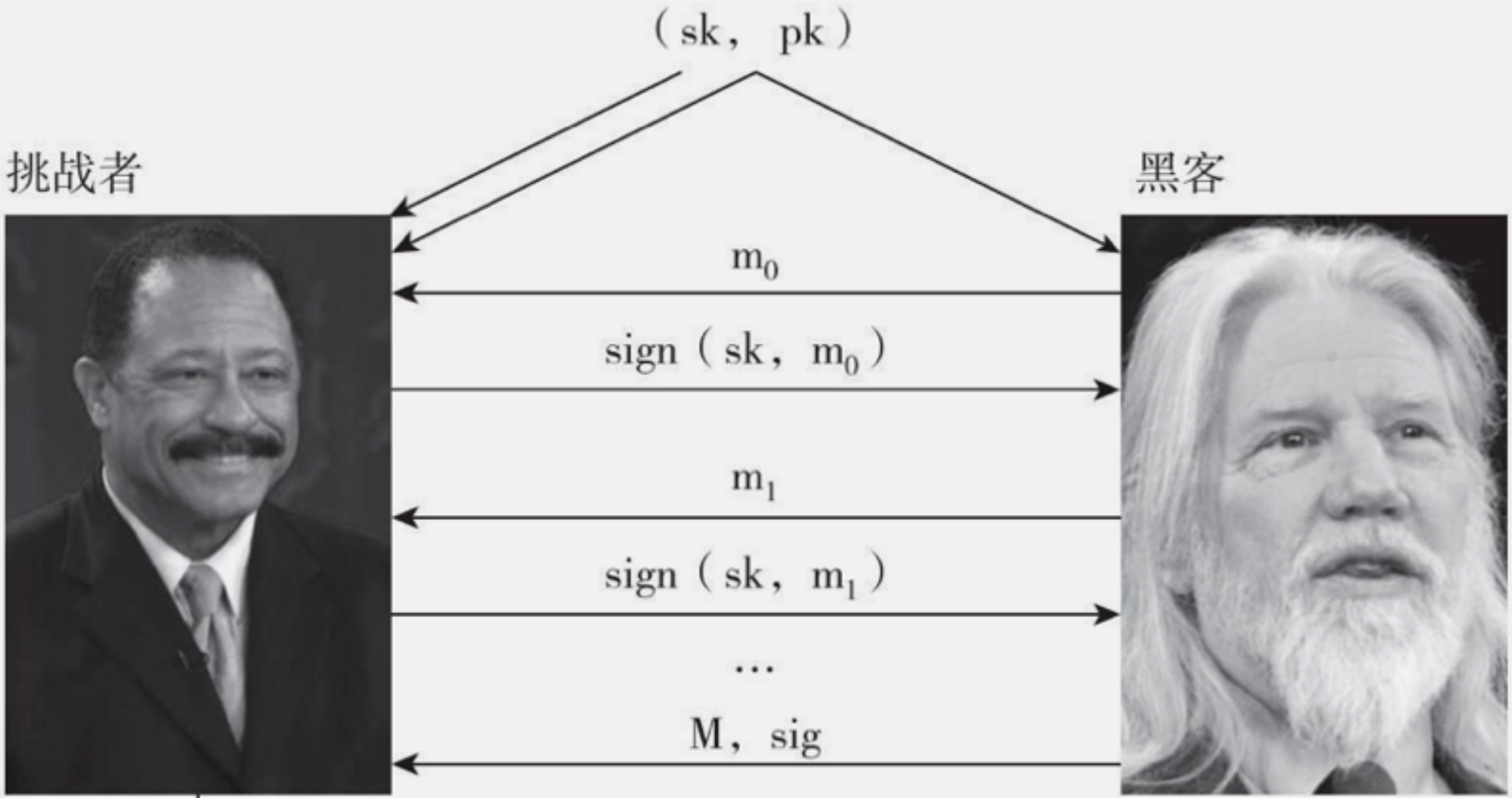


O(log n)

数字签名

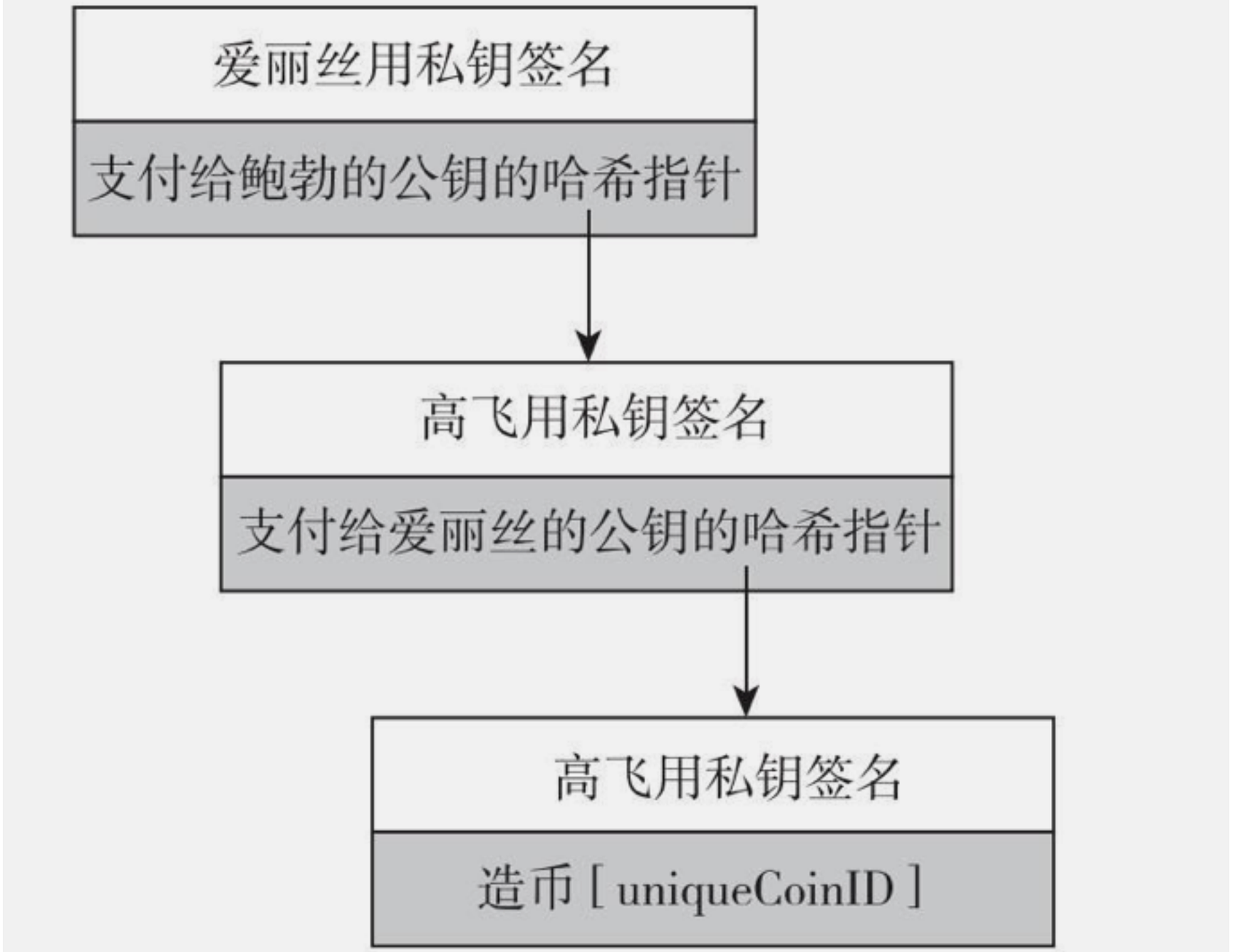
- 自己签名，任何人均可以验证
- 公钥和私钥
- 不可伪造
- 信息大小

不可伪造游戏

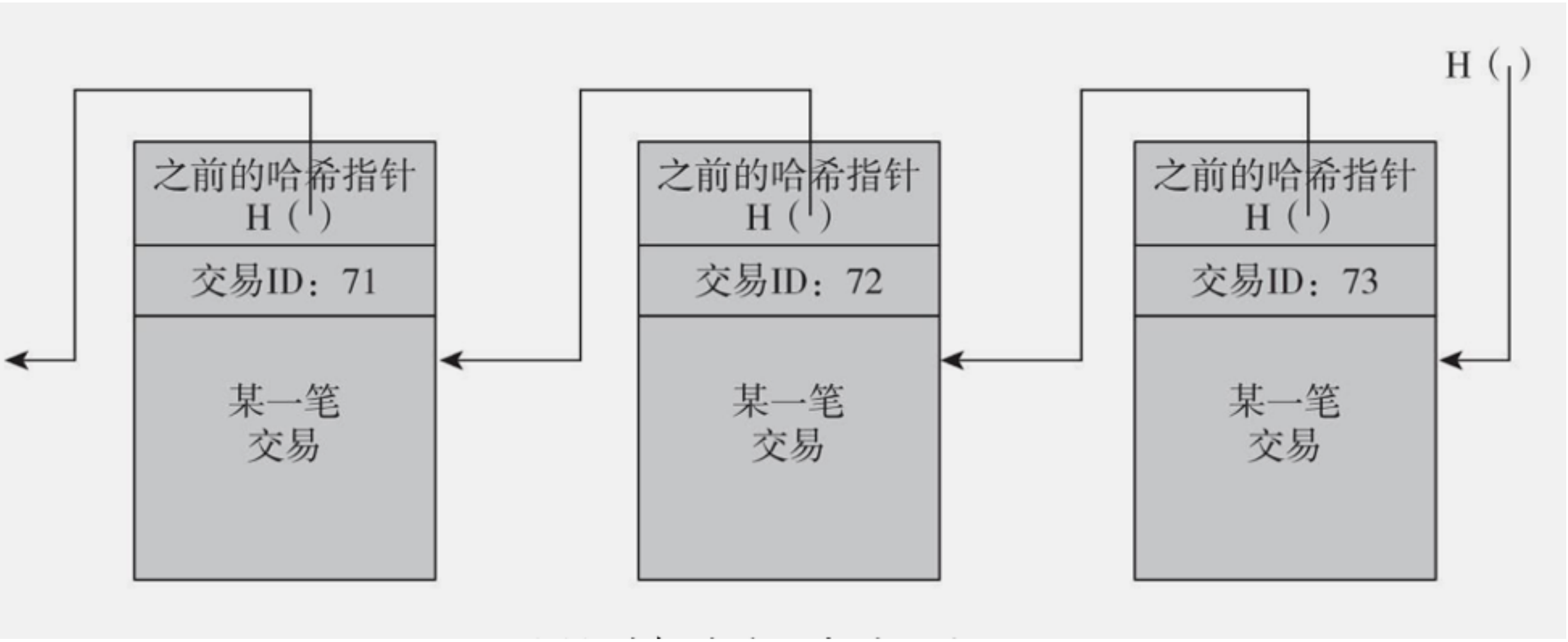

(sk, pk)
挑战者
黑客
m_0
sign(sk, m_0)
m_1
sign(sk, m_1)
...
M, sig
verify(pk, M, sig)
M not in {m_0, m_1, ...}
如果是正确的，黑客赢得这个游戏

公钥即身份

高飞币


爱丽丝用私钥签名
支付给鲍勃的公钥的哈希指针
高飞用私钥签名
支付给爱丽丝的公钥的哈希指针
高飞用私钥签名
造币 [uniqueCoinID]

贪心币


之前的哈希指针
H ( )
交易ID：71
某一笔
交易
之前的哈希指针
H ( )
交易ID：72
某一笔
交易
之前的哈希指针
H ( )
交易ID：73
某一笔
交易
H ( )

贪心币

交易ID：73		类型：造币
被创造的货币		
序号	数量	造币记录
0	3.2	0x…
1	1.4	0x…
2	7.1	0x…

虚拟货币ID 73（0）

虚拟货币ID 73（1）

虚拟货币ID 73（2）

贪心币

交易 ID：73		类型：付币
消耗的虚拟货币 ID： 68（1），42（0），72（3）		
被创造的货币		
序号	数量	造币记录
0	3.2	0x…
1	1.4	0x…
2	7.1	0x…
签名		

谢谢！

孙惠平

sunhp@ss.pku.edu.cn